Safety Science 127 (2020) 104698

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/safety

# Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech Republic

David Rehak[a,*], Martin Hromada[b], Tomas Lovecek[c]

[a] VSB – Technical University of Ostrava, Faculty of Safety Engineering, Czech Republic
[b] Tomas Bata University in Zlín, Faculty of Applied Informatics, Czech Republic
[c] University of Žilina, Faculty of Security Engineering, Slovakia

ARTICLE INFO

*Keywords:*
Critical infrastructure
Electric power
Personnel threats
Effects
Security solutions and measures

ABSTRACT

The Electric Power Infrastructure Sector is a uniquely critical sector among other critical infrastructures. Disruptions to or failures of its functions would result in extensive effects, not only on society itself but also on all of the (other) dependent critical infrastructure sectors. The key areas of electric power supply systems that demonstrate the greatest vulnerability to terrorist attacks include the following areas of vulnerability: physical vulnerability, cyber vulnerability and personnel vulnerability. Considerable attention is devoted to the problems and issues of external anthropogenic threats (e.g. terrorism). Internal intentional anthropogenic threats represent an almost neglected sector in the field of security research. Based on this fact, this article studies the issues of threats to and by personnel in the electric power critical infrastructure sector and their influence and effect on dependent critical infrastructure sectors. Attention is especially given to defining these threats and their (further) categorization into two groups: physical and cyber threats. Equally, this article also highlights the impacts of personnel threats in dependent critical infrastructure sectors. The main part of this paper focuses on security measures that can be used to minimize the potential impact of personnel threats. This especially concerns (1) assessing the resilience of elements in the electric power critical infrastructure sector to personnel threats, (2) defining the requirements for personnel security, and (3) the use of standard technical and innovative technologies to monitor and assess the activities of authorized or non-authorized persons.

## 1. Introduction

The critical infrastructure system (CIS) can be divided into two areas according to its functional specificities: technical and socio-economic infrastructures (Rehak et al., 2016). A considerable interdependence exists between these infrastructure areas. All sectors of the socio-economic area require the unlimited possibilities of disposing services to technical infrastructure sectors, and by contrast, technical infrastructure sectors are—in the case of a crisis situation—fully dependent on the services of socio-economic sectors. Both fields, however, have a clear dependence on the energy sector, which, on this basis, is rightly referred to as *uniquely critical* (PPD-21, 2013).

Electric power critical infrastructure (EPCI) represents a highly complex network-based system that includes the generation, transmission and distribution of electricity. As a consequence of their diversity, their elements are continually threatened by several major high intensity security threats. The most significant and hostile threat of a global nature can clearly be considered the impact of climate change (Mikellidou et al., 2018). However, in addition to global threats, EPCI elements are also exposed to regional threats. The most important regional threats are currently considered meteorological phenomena (Ward, 2013) and terrorism (Morgan et al., 2012).

Today, the greatest vulnerability of EPCI elements is related to terrorism—threats that can be very difficult to predict and whose effects cause extensive blackouts. An author team from the U.S. National Academy of Sciences has published studies of three key areas of the electrical power supply system that show the greatest vulnerability to terrorist attack (Morgan et al., 2012). These areas include physical vulnerability, cyber vulnerability and personnel vulnerability.

Several research projects (e.g. APENCOT, CIPnES, PACITA, CIPAC) and expert publications (e.g. Garcia, 2007; Jang et al., 2009; Lovecek et al., 2010) have been conducted in order to protect critical elements from external intentional anthropogenic threats (i.e. physical or cyber threats). European research into protecting critical elements from internal intentional anthropogenic threats (i.e. personnel threats) in the energy sector is virtually non-existent, however.

* Corresponding author at: Lumirova 13, 700 30 Ostrava-Vyskovice, Czech Republic.
*E-mail address:* david.rehak@vsb.cz (D. Rehak).

https://doi.org/10.1016/j.ssci.2020.104698
Received 20 December 2018; Received in revised form 1 November 2019; Accepted 1 March 2020
Available online 10 March 2020

Based on this fact, the aim of this paper is to present current personnel threats in the electric power critical infrastructure and their impacts on the dependent sectors and to formulate a possible approach to assess the resilience of the electric power critical infrastructure elements to these personnel threats. Following this assessment approach, the aim of the article is to define recommended measures to minimize personnel risks in the critical infrastructure system with a focus on procedural, cultural and technical measures.

## 2. Electric power critical infrastructure

The electricity grid is a very complex and interconnected network for the production, transmission, transformation and distribution of electricity. It includes electricity connections and direct power lines, the equipment for measuring, protecting, controlling and signalling information, and telecommunication systems. Power grids provide electricity to billions of individuals around the world, often with over 99.9% reliability. Residents of most countries rely on the high reliability of this service.

A massive disruption to electricity supply would result in the disruption of vital services (e.g. water supply, emergency and health services), which could even lead to social unrest. An example might be 1977, when a power outage in New York led to widespread riots and the subsequent arrest of more than 3000 individuals for illegal offenses (Brown-Cohen, 2010).

Electrical energy infrastructure is one of the key infrastructure subsectors in the European Union and includes electricity generation and transmission infrastructure and facilities (European Council, 2008). In the Czech Republic, the energy sector is governed by the Energy Act (Act 458, 2000) and in addition to the above-mentioned infrastructure, includes components for electricity distribution to consumers.

The basic principle of **electricity generation** is the conversion of primary energy into electricity. Power plants categorized into thermal, nuclear or renewable energy (i.e. water, wind and solar power) are used for this purpose. The following can be categorized from the point of view of production (Act 240, 2000) among the most important electricity critical infrastructure sector elements:

(a) A power plant with a total installed capacity of 500 MW or more,
(b) An operator providing supporting services with a total installed capacity of 100 MW or more,
(c) Power lines for distributing power and securing power generation,
(d) An electricity distribution dispatching system.

The transmission of electricity in the form of very high voltage is provided through the **distribution and transmission system**. For long-distance transmissions, voltage is transformed into very high voltage at a power plant and achieves values of 110 kV, 220 kV, 400 kV or 800 kV. The transmission system infrastructure consists of transformers, cable masts, cables (conductors), compensating elements and control and protection elements. The most important elements of critical infrastructure in the energy sector can be ranked in terms of the transmission system (Act 240, 2000):

(a) A transmission system with a voltage of at least 110 kV,
(b) A power station transmission system with a voltage of at least 110 kV,
(c) Technical dispatching control of the transmission system by an operator.

Very high voltage is then transformed into 35 kV or less and distributed through the **distribution system** to its final consumers. The most important critical electricity infrastructure sector elements can be also ranked in terms of distribution (Act 240, 2000):

(a) 110 kV (i.e. 110/110 kV, 110/22 kV and 110/35 kV 110/35 kV) lines and power lines for the 110 kV distribution system and 110 kV power lines are assessed according to their strategic importance in the distribution system,
(b) Technical dispatch of the distribution system operator.

Based on the results of a vulnerability analysis the above-mentioned elements (Deloitte Advisory, 2017; MIT, 2014), the **main vulnerability of critical technical infrastructure** elements includes the main and back-up technologies of the transmission system operator and the most vulnerable elements of the power-generation critical infrastructure. This dispatching system allows the transmission system substations to be controlled remotely and automatically compensates for variances between the generation and consumption of electricity. It also allows the flow of electricity flows and voltage levels in the transmission system to be controlled. **Critical situations related to this technical dispatch centre** include:

- Programmable manipulations, based on the daily preparation of network operations,
- Frequency regulation and power balance,
- Nodal area power coordination,
- Managing the activation of “bought-in” from support services,
- Exploiting the electrical energy balancing market,
- The purchase of regulatory energy and use of emergency assistance from abroad,
- Voltage and reactive power regulation,
- Monitoring of transmission systems,
- Resolution of eventual transmission system failures,
- Coordination of operations with foreign Transmission System Operators (TSOs),
- Detection of bottlenecks,
- Remote control of power supply elements,
- The use of system operation prediction models,
- The use of the higher dispatching control system functions, for example, network calculations, re-dispatching, reconfiguration, contingency analysis, etc.,
- Keeping operational records and documentation of all processes, including failures,
- Processing event and fault records,
- Performing network calculations,
- Conducting tests,
- Collecting, processing and archiving data from the transmission system.

All these activities are linked to other major distribution and transmission system operators, including at the international level. Basic entities that share significant links can therefore be considered (Deloitte Advisory, 2017):

- Dispatchers of technical dispatching centres or power plant personnel,
- Distribution system dispatchers,
- Neighbouring transmission system operators’ dispatchers,
- The operation of locally controlled substations and permanent staff services,
- Business partners providing regulatory energy supplies to and from abroad.

On the basis of the points above, it is clear that personnel security and security issues themselves are crucial, even from the point-of-view of ensuring the continuity of society and other elements of European critical infrastructures. The following text therefore analyses the current security threats related to critical power infrastructures.

**Table 1**
Current security threats to electric power critical infrastructure.

| | Naturogenic | Technogenic | Anthropogenic |
|---|---|---|---|
| External threats – global | Climatic threats<br>Raw material threats | (X) | Conflict/War threats |
| External threats – regional | Meteorological threats<br>Geological threats<br>Biological threats | Cascading threats | Physical threats<br>Cyber threats |
| Internal threats | (X) | Process and technological threats | Personnel threats |

## 3. Current security threats to electric power critical infrastructure

Elements of electrical energy critical infrastructure are continuously exposed to threats of varying nature and intensity. These threats can be categorized according to their area of activity into three groups. The first group consists of external threats of a global nature. This group of threats cannot be effectively affected or minimized. The second group is external threats of a regional nature. These threats also cannot be affected, but at least in terms of elements of EPCI a sufficient level of resilience can be built against their effects. The final group is internal threats. This group of threats can be considerably affected by the previous groups, mainly by applying effective security measures. An overview of current security threats affecting the EPCI is presented in Table 1.

One group of external threats of a global nature comprises only naturogenic and anthropogenic threats. Naturogenic threats are especially climatic and raw material threats, while anthropogenic relates to Conflict/War threats. **Climatic Threats** relate to climate change on the Earth and its global impacts such as global heating, drought, precipitation, rising sea-levels and extreme events such as floods, storms, hurricanes and blizzards (Mikellidou et al., 2018). **Raw Material Threats** relate to the use of natural resources in the functioning of EPCI. These include, for example, lack of water or mineral resources.

The external threats group includes threats of a regional nature or naturogenic threats, (e.g. meteorological, geological and biological), technogenic threats, (i.e. threats arising from the cascade of effects in a critical infrastructure system) and anthropogenic threats, (i.e. physical and cyber). **Meteorological Threats** relate to negative phenomena in the atmosphere, such as strong winds, storms, hurricanes and snow disasters (Ward, 2013). **Geological Threats** relate to negative phenomena in the geosphere, such as earthquakes, volcanic activity or landslides. **Biological Threats** relate to the spread of harmful viruses and bacteria that may cause epidemics, pandemics or epizootics. These threats are not directly related to infrastructure, rather to people associated with it. Another significant group is **Cascading Threats**, which are threats arising from cascading effects within a critical infrastructure system (CIS). The risk is especially related to dependent elements, specifically elements dependent on electricity power supplies (Rehak et al., 2016). **Physical Threats** are intentional anthropogenic behaviour from external environments, for example, acts of terrorism or criminal activity (Morgan et al., 2012). **Cyber Threats** are related to the deliberate disruption of information and communication systems in a critical infrastructure element. The most famous case in recent years was the cyber-attack on Ukraine's energy network (Knake, 2017).

The group of **Internal Threats** adversely affecting the performance of CIS include process and technology threats and personnel threats. **Process and Technology Threats** include technological breakdown of the affected elements, for example, radiation accidents, dangerous chemical leaks, extensive civil engineering disruptions and water-distribution and water resource related accidents. The biggest power infrastructure disruption ever occurred in 2005—the Java-Bali blackout (BBC, 2005). Its cause was a technical failure in one of the power lines that subsequently spread like domino effect to the distribution system stations, resulting in several power plants being disconnected from the grid.

**Personnel Threats** are situations when an employee or other authorized person is a risk factor. These threats can be further categorized into **unintentional** and **intentional** (Morgan et al., 2012). **Unintentional Personnel Threats** include an insufficient awareness of security, insufficiently qualified personnel or human error. The most famous example is the Chernobyl nuclear power plant accident in 1986, which occurred as a result of the insufficiently attempted and inadequately competent personnel (NEI, 2015). By contrast, intentional personnel threats are for the purpose of, for example, personal enrichment, revenge or achieving ulterior goals (i.e. the essence of terrorism).

## 4. Personnel threats in electric power critical infrastructure

The starting point for defining personnel threats to electrical energy critical infrastructure was analysing and assessing the current level of risk from the perspective of critical infrastructure entities (i.e. operators or owners) in the context of personnel security at critical infrastructure elements (Deloitte Advisory, 2017). The analysis clearly showed a long-term absence of a certain communal approach, which would, also from a terminological point of view, express the same level of threat in the area. Equally obvious is the absence of a common, and to a certain extent, universal catalogue of risks for the generation, transmission and distribution of electricity.

An outcome of this unsatisfactory situation was a catalogue of basic categories of personnel threats in EPCI according to the analytical work of security research projects (Table 2).

Key risks were subsequently identified in each category, analysed and evaluated. The methodological basis was the RISKAN risk analysis support tool (2015), which allows a semi-quantitative risk assessment. The Risk Ratio ($R$) is thus determined as the product of the point values of the following variables: asset value ($A$), asset vulnerability ($V$), and probability of threat failure ($P$). It should be noted that the value of the asset (i.e. potential impact) is based on selected criteria for identifying and determining critical infrastructure elements, for example, the number of people killed or injured, economic impacts or the effects on society's quality of life (European Council, 2008).

All variables were rated from 1 (representing a low asset value, asset vulnerability or likelihood of threat) to 5 points (representing a high asset value, asset vulnerability or likelihood of threat). Table 3 shows the results of a practical risk analysis, and the categorization of risks is to some extent a generalization of the analysis results preceded by the semi-quantitative risk assessment. The outcome of this evaluation differentiated the risks according to the numerical values obtained.

The final result of assessment was the creation of a comprehensive yet generally compiled personnel risk catalogue (Table 3), whose principle is the classification of risks into three levels (RISKAN, 2015):

- Critical risks (Red), reaching 71 or more points,
- Unacceptable risks (Yellow), reaching values of 41 to 70 points,
- Acceptable risks (Green), reaching values of 1 to 40 points.

**Table 2**
Categories of personnel threats in electric power critical infrastructure.

| Physical threats | Cyber threats |
|---|---|
| Physical theft | Data breaches |
| Physical loss | Ransomware |
| Physical damage | Information leakage |
| Injury | Identity theft |
| Threatening | Cyber espionage |

**Table 3**
Catalogue of personnel risks in electric power critical infrastructure.

| Index | Risk | Index | Risk | Index | Risk |
|---|---|---|---|---|---|
| 1 | Inappropriately determined workflows | 13 | Unauthorized access to TSFO elements | 25 | Bomb threats – written |
| 2 | Failure to observe workflows | 14 | Unauthorized manipulation of TSFO elements | 26 | Threats to TR and permanent services |
| 3 | Employee operational errors | 15 | Intentional damage by employees | 27 | Threats – other |
| 4 | Third-party employee errors | 16 | Sabotage by employees | 28 | Extortion of employees |
| 5 | Incorrect manipulation of TSFO elements | 17 | Impersonation of third-party employees' physical identities | 29 | Hostage situations |
| 6 | Ignorance, lack of employee preparedness | 18 | Destruction of cooling equipment | 30 | Kidnapping employees |
| 7 | Ignorance, lack of employee preparedness | 19 | Destruction of outdoor power lines | 31 | Letters and parcels with dangerous contents |
| 8 | Lack of material resources | 20 | Destruction of outdoor power transmission poles | 32 | Use of toxic agents |
| 9 | Lack of human resources | 21 | Destruction of workspaces or parts thereof | 33 | Destruction or elimination of technological workspaces for data processing and transmission |
| 10 | Security service failures | 22 | Use of a weapon | 34 | Destruction or elimination of continuous services |
| 11 | Acquiring information about site protection measures | 23 | Demonstrations occurring near sites | 35 | Destruction or elimination of dispatching centres |
| 12 | Impersonation of a user | 24 | Bomb threats – by phone or e-mail | | |

Table 3 is also a type of intersection of partial analysis results and can also be considered a result of understanding the sector and perceiving its risks (i.e. generation, transmission and distribution of electricity). It can be generally stated that the table presents and considers the risks sorted according to intentional or unintentional human error.

The presented risk catalogue is to some extent a generalization of ascertained facts, even with regard to the requirements of operators and owners of critical infrastructure. Generalization reflects the need to reduce the sensitivity of data presented in relation to their practical size and potential impact on security and resilience.

This catalogue has been verified by leading domestic and foreign electricity companies and subsequently discussed with and approved by the Ministry of Industry and Trade of the Czech Republic. From the results of this catalogue, concrete assessments of the **resilience of critical energy infrastructure elements with regard to personnel threats can be achieved** (section 6). If specific weaknesses are identified in the resilience assessment, some of the **recommended measures for minimizing personnel risks** should be applied and implemented (section 7).

## 5. Impact of personnel threats on dependent sectors

Personnel threats in the electricity generation sector, especially intentional threats, pose a serious risk to the critical infrastructure system. The effects of these threats are undesirable events that result in disruptions or even temporary failures in the performance of the given element that can lead to large power outages. A cascade effect may also occur in the critical infrastructure system (Rinaldi et al., 2001) in which the disruption of power supply causes the disruption or failure of dependent elements across all sectors (Fig. 1).

From Fig. 1 above, it is clear that critical infrastructure represents a very closely interconnected system. This potentially could lead to the occurrence of extensive cascade effects. In the case of disruption to power supply, the first line represents a **primary impact** (red) on dependent sector elements. These impacts may demonstrate different intensities, the greatest of these affecting water supply, health services, information and communication systems, financial markets and currencies elements and public administration. By contrast, the food industry and agricultural sector will not be as greatly affected (Oulehlova, 2017).

**Secondary impacts** (orange) – these impacts provide equally varying degrees of intensity. The greatest of these effects are on financial markets and currency sectors, emergency services, public administration and transport sectors.

**Tertiary impacts** (purple) – disruption to power distribution will spread, for example, because of distortion in the transport sector's elements. The impacts with the greatest intensity will affect emergency services, health services, water supply services, the food industry and agricultural sectors. Power supply disruption will occur, for example, as a result of outages in information and communication system elements.

Beside the effects of power supply disruptions and in addition to cascading effects, the critical infrastructure system also can be affected by **Synergistic Effects**. These entail the added effects of combined interactions and thus increase the sum of the impact (Rehak et al., 2016). An example of this may be the mutual effects of the primary, secondary and tertiary impacts of power supply disruption to emergency services elements.

In this case, the cumulative impact of disruptions to power supply, information and communication systems and traffic will be greater than the individual impacts. Secondary impacts (orange) – power supply disruptions will occur, for example, because of outage of information and communication system components. These impacts also show different degrees of intensity. The greatest intensity relates to financial and currency markets, emergency services, public administration and transport sectors. Tertiary impacts (purple) – power supply disruptions will occur, for example, because of distortion to the elements of the sector to the right. The impacts with the greatest intensity will then affect elements of the emergency services, health services, water supply, food industry and agriculture.

## 6. Assessment of the resilience of EPCI elements to personnel threats

An important factor in the functionality of EPCI elements is their resilience to disruptive events (i.e. the negative impact of threats on these elements). In the critical infrastructure context, resilience is understood as *the ability to reduce the magnitude, impact, or duration of a disruption. The effectiveness of a resilient infrastructure depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event* (NIAC, 2009). According to this, it can be stated that the resilience of critical infrastructure elements is determined by three basic components: (1) robustness (ensuring the absorption

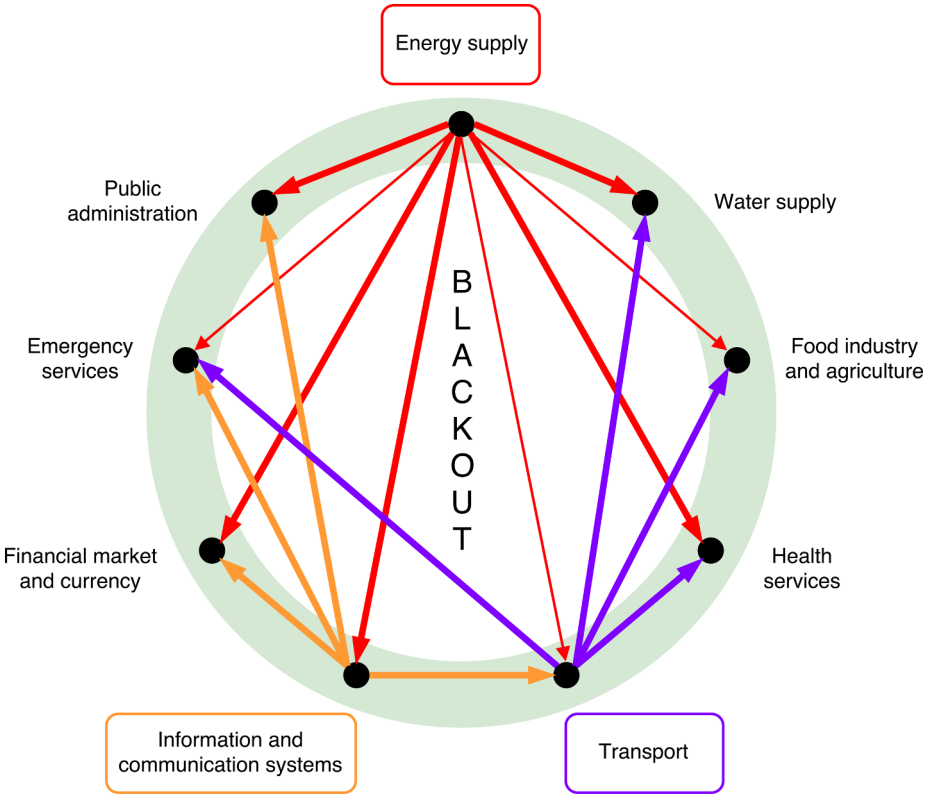


**Fig. 1.** Dependence of critical infrastructure sectors on electric power supply.

capacity of the element), (2) recoverability (ensuring the rapid recovery potential of the element) and (3) adaptability (ensuring the adaptation potential of the element to disruptive events already occurring).

The term resilience was first defined by Holling (1973) in connection with the resistance and stabilization of ecological systems (later socio-ecological systems). In this context, resilience can be understood as *measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables*. The difference between the resistance and the resilience of ecosystems was subsequently defined by Sugden (2001): *The "resistance" of an ecosystem to a perturbation, such as the introduction of an alien species, is a measure of how much the system changes. Its "resilience" is the extent to which it can recover after the source of change is removed.*

In this context, it can be stated that the resistance of critical infrastructure ensures that no disruptive event occurs. It is therefore a preventive measure, namely crisis preparedness and physical resistance of the infrastructure. While the essence of critical infrastructure resilience is to dampen the impact of an already occurring disruptive event and the subsequent recovery and adaptation of the infrastructure to that event. However, at present, resistance in the context of critical infrastructure is not defined separately but is seen as part of the robustness absorption capacity (NIAC, 2009).

Assessing the resilience of EPCI to personnel threats can be considered a significant preventive measure that leads to the early identification of weaknesses or even vulnerable locations. Resilience assessment is based on the semi-quantitative assessment of twelve key areas (Rehak et al., 2019):

- Crisis preparedness, physical resistance, redundancy, detection capability and responsiveness (determining the robustness of the element),
- Material resources, financial resources, human resources and recovery processes (determining the element's recoverability),
- Risk management, innovation processes and education and development processes (determining the element's adaptability).

A set of measurable items was created for each area in order to identify the current element's resilience to personnel threats according to different variants. Examples of measurable items and their variants for "robustness/crisis preparedness" is presented in Table 4.

The point rating presented in Table 4 is based on the principle of linear ascendancy, in which the difference between individual point values is directly proportional. In practice, for example, this means an increase from 1 to 2 is the same as an increase from 4 to 5. The value of this increase is 20%. This principle is also valid in cases where the assessment scale includes three values, for example, 1, 3 and 5. In this case, the increase of value between 1 and 3 and between 3 and 5 is 40%.

In the final stage of assessing the resilience of EPCI elements, an assessment of the individual measurable variables is required. These variables are assessed at:

- **High level of resilience (5):** measurable variables in this category have excellent parameters that determine a high level of element resilience and therefore no further action is required.
- **Acceptable level of resilience (4):** measurable variables in this category provide very good parameters that can be improved but are not essential for overall element resilience.
- **Low level of resilience (3):** measurable variables in this category provide sufficient parameters although improving the resilience of the element to personnel threats is expected.
- **Insufficient level of resilience (2):** measurable variables in this category show very poor parameters that significantly reduce element resilience to personnel threats.
- **Critical level of resilience (1):** measurable variables in this category either completely fail or show a critically low level of parameters. These items need to be completely revised, established or restored as soon as possible.

**Table 4**
Measurable items for assessing the robustness (crisis preparedness) of EPCI elements to personnel threats (Rehak et al., 2018).

| Measurable items | Description | Points evaluation |
|---|---|---|
| Responsibilities, obligations, powers | The aim is to assess the extent to which the responsibilities, obligations and powers of roles involved in administrative activities have been defined. | **5**: These are defined for all administrative activity roles.<br>**3**: These are defined for selected administrative activity roles.<br>**1**: No defined administrative activity roles. |
| Employee scrutiny | The objective is to assess whether the following has occurred:<br>– The definition of conditions for scrutinizing information about job seekers (availability of two good references, checking the candidate's CV, verification of education and qualifications, independent identity verification).<br>– The definition of procedures for verifying an employee's reliability.<br>– The definition of regular reviews of all employees' work.<br>– The detection of dissatisfaction/personal/financial problems that may lead to errors or other security implications. | **5**: All criteria were met.<br>**4**: The first three criteria were met.<br>**3**: Two criteria were met.<br>**2**: One criterion was met.<br>**1**: None of the criteria were met. |
| Data protection agreements | The aim is to assess whether defined procedures are in place to ensure the data protection contract is signed (e.g. confidentiality agreements, contract of employment, etc.) where necessary. | **5**: Data protection is addressed in each signed contract.<br>**3**: Data protection is addressed in selected contracts.<br>**1**: Data protection is not addressed in signed contracts. |
| Employment activity performance conditions | The aim is to assess whether the content of the provisions on data protection, the obligations of beneficiaries, which should last for a certain period of time after termination of the employment relationship, and the steps in non-compliance are described and established. | **5**: Relationships with employees are defined by data protection provisions, even after termination of employment, and breaches are described as non-compliance.<br>**3**: Relationships with employees are defined by data protection provisions, non-compliance steps are described.<br>**1**: No data protection provisions are defined in relation to the employee. |
| Employee training | The aim is to assess whether:<br>– The definition of mandatory security training is established.<br>– The definition of training content (inclusion of security requirements and legal responsibilities) and description of relevant control mechanisms exist.<br>– Evidence of trained staff and regular training. | **5**: All criteria were met.<br>**3**: Two criteria were met.<br>**1**: No criteria were met. |
| Personnel management | The aim is to determine whether:<br>– Personnel management is specifically resolved in the subject's security plan.<br>– The facility has appointed a security manager to manage the personnel security process.<br>– Security managers are aware of the procedures for requesting approval and authorization of access.<br>– Initial and annual safety awareness training is provided to all employees.<br>– Training records are archived.<br>– The entity has a comprehensive personnel security policy.<br>– Local audits are performed on a regular basis in order to ensure that personnel security is in line with the security policy.<br>– Directors or security managers are immediately informed about security incidents that may have an influence on verifying personal identity.<br>– The security manager knows what steps should be taken when defamatory and misleading information about an individual is received.<br>– A register of access is available. | **5**: All criteria were met.<br>**4**: 8/10 criteria were met.<br>**3**: 5/10 criteria were met.<br>**2**: 3/10 criteria were met.<br>**1**: Less than 3 criteria were met. |
| Personnel reliability | The aim is to assess whether:<br>– The reliability of personnel is a component of the given subject's security plan.<br>– All employees underwent the process of reliability controls before they have access to selected assets.<br>– Induction training and certificates of completion were passed on to employees prior to being allowed access to selected assets.<br>– The employee signed a commercial confidentiality agreement prior to gaining access to the selected assets.<br>– All employees with unauthorized access to selected assets have been screened and verified, and access has been restricted. | **5**: All criteria were met.<br>**4**: 4/5 criteria were met.<br>**3**: 3/5 criteria were met.<br>**2**: 2/5 criteria were met.<br>**1**: Less than 2 criteria were met. |
| Human resources management | The objective is to assess whether:<br>– Human resources management is specifically resolved in the subject's security plan.<br>– All employees are required to complete the control checklist on application and prior to recruitment.<br>– A principle is in place to ensure all employees who require access to selected assets are monitored.<br>– Employees are assigned to positions with specific access rights.<br>– Each employee position is associated with a record of potential risks.<br>– All positions are designated with the correct safety classification.<br>– Minimum educational training and examination criteria are set for those responsible for physical safety.<br>– Pre-employment screening processes prior to the acceptance of selected persons include checks on relevant links, previous employment record, education, professional training and professional certificates. | **5**: All criteria were met.<br>**4**: 4/5 criteria were met.<br>**3**: 3/5 criteria were met. |

(*continued on next page*)

**Table 4** (*continued*)

| Measurable items | Description | Points evaluation |
|---|---|---|
| | | **2**: 2/5 criteria were met.<br>**1**: Less than 2 criteria were met. |

Note: The measurable items in Table 4 apply only to the crisis preparedness which is a subgroup of robustness. It is therefore a preventive measure representing the resistance of a critical infrastructure element. For this reason, these measurable items have no meaningful value about absorbing the effects of a disruptive event or subsequent recovery and adapting a critical infrastructure element to that event.

**Table 5**
Personnel security requirements.

| Area | Requirements |
|---|---|
| Responsibilities, obligations and powers | – The definition of obligations and powers for roles associated with administrative activities. |
| Employee security clearance | – The definition of security reliability scanning procedures, (e.g. the availability of two sufficient references, checking the candidate's CV, verifying education and qualifications, independent verification of identity).<br>– The definition of a procedure for verifying employee reliability.<br>– The definition of regular employee obligations and performance reviews.<br>– The definition of a procedure for providing information about private circumstances that could lead to mistakes or have other security implications (frequent absence, stress, depression, personal and financial problems, behavioural and lifestyle changes, etc.). |
| Data protection agreements | – The definition of a procedure for signing a data protection agreement, (e.g. employment contract confidentiality agreements, etc.) where necessary. |
| Work performance conditions | – The definition of providing data protection content. The obligation of authorized persons should endure for some time after the termination of an employment relationship, and steps should be established for situations when conditions are not met. |
| Staff training | – The definition of mandatory security training.<br>– The definition of training content for security requirements, legal responsibilities and relevant control mechanisms, including descriptions and summaries.<br>– Trained staff and regular training records. |
| Reactions to security incidents and failures | – The definition of procedures for reporting security incidents and vulnerabilities. |
| Disciplinary processes | – The definition of procedures for violations of security measures or non-compliance with the organization's work practices. |
| Termination of the employment relationship | – The definition of procedures for returning assets held by employees, registration.<br>– The definition of procedures for removing access permissions. |

## 7. Recommended measures for minimizing personnel risks in critical infrastructures

Based on identifying specific personnel risks (Table 3) and the results of the EPCI element resilience assessment, adequate measures can be applied to minimize risk. These measures are categorized into three groups: **procedural, cultural and technical measures**. Procedural measures consist of defining the personnel security requirements. Cultural measures establish the need and responsibility for the security of the entrusted property. Technical measures include the use of standard technology for monitoring and evaluating the activities of authorized persons (i.e. use of intruder and hold-up alarm systems and systems using GPS localization) and the development of innovative technologies. In addition to the above-mentioned measures, this section introduces new technologies that have been developed from recognizing discrepancies in the behaviour of individuals in real-time through deep structured learning methods.

It is important to acknowledge that the source of personnel threats (intentional and unintentional anthropogenic threats) are those individuals with process or access rights (i.e. the logical or physical approach). It is very important to be aware of persons with specific privileges. Not every employee of an organization (or employees of a supply or customer organization) represents an internal personnel threat to all of the organization's processes and services. For example, a maintenance employee has access to a distribution transformer but no access to the data centre, while for a data analyst, the situation is reversed. The maintenance employee will therefore be an internal personnel threat in relation to the distribution transformer, but for the data centre, they will be an external threat (physical or cyber). Analogously, this is also be valid for the data analyst.

### *7.1. Procedural measures*

The essence of implementing procedural requirements is defining the requirements of **personnel security**. This area has been defined under a comprehensive or integrated protection management system based on analysis and consultation with relevant authorities in the critical infrastructure field. It is also perceived as a system for selecting individuals with regard to access to the subject's information assets, verification of access to information assets, training and protection. The requirements focus on minimizing the impact of human error, potential theft or fraud or misuse of the organization's information assets. With regard to creating these personnel security requirements, the following areas are seen as with special interest:

- Responsibilities, obligations and competencies,
- Employee screening,
- Data protection agreements,
- Work performance conditions,
- Staff training,
- Response to security incidents and failures,
- Disciplinary processes,
- Response to security incidents and failures,
- Termination of the employment relationship.

Specific requirements for individual areas in personnel security are presented in Table 5.

The creation of a purposeful and effective preventive measures system against internal intentional personnel threats requires an awareness of a certain oxymoron: the more we trust a person (give them certain competencies), the more we should not trust them (e.g. unauthorized behaviour). This approach should be applied throughout the employment lifecycle of the eligible person, specifically from the moment an authorization is granted (e.g. selection procedures or workload allocations) to when it is rescinded (e.g. termination of employment) or even for some time after it is rescinded.

### 7.2. Cultural measures

The term safety culture was first used in 1986 by a group of International Atomic Energy Agency workers after the Chernobyl nuclear reactor accident (IAEA, 1991). The investigative team surveying the accident concluded that the main reason for the reactor overheating were deficiencies associated with the organization's safety culture. After this event, safety culture was at the centre of interest for optimizing the impact of corporate culture on employee behaviour in relation to security.

Several prominent authors have devoted themselves to defining safety culture and safety climate over the past 30 years (e.g. Cox and Cox, 1991; Hale, 2000; Mohamed, 2003; Halaj et al., 2018). These authors consistently argue that safety culture reflects the attitudes, beliefs, perceptions and values that employees share in relation to safety. These attitudes, beliefs and perceptions that organizations define as norms and values affect their actions and responses to risks. Safety culture is therefore influenced by the unconscious behaviour of the organization's employees in safety matters.

Without achieving the necessary security awareness, individuals cannot fully perform their tasks, thereby disrupting the whole system. New risks and threats confirm the importance of building individual security awareness, as a lack of security awareness can be considered a threat (Brvnistan, 2016).

### 7.3. Technical measures

The personnel security requirements defined above cover the entire lifecycle of the involvement of employees in an organization. However, it is appropriate, even necessary, to implement certain technical measures in order to ensure that certain requirements are met. These include, for example, requirements such as defining the routine monitoring of all employee work performance, defining employee reliability check procedures, or defining security incident and weaknesses reporting procedures.

In the course of their usual activities, authorized individuals can move around in normal physical space or cyber space. **Technical measures for standard monitoring of persons in a given physical space** have long made use of surveillance systems such VSS/CCTV systems, ACS systems or I&HAS, or more recently, GPS-based systems. Software and hardware solutions can now be employed to monitor and regulate the activities of authorized persons in a virtual space through logs that record all activity. An overview of technical resources for monitoring and evaluating authorized persons in virtual and physical space is presented in Table 6.

All of the above-mentioned technical measures allow the activities of authorized persons to be monitored and evaluated. The common disadvantages of these measures are their ability to react after or imminently prior to an undesirable event. One of the standard measures that would, with sufficient lead time, expose the intended intentions of an authorized person well in advance is a polygraph test. However, this solution is accompanied by pitfalls involving capacity, legal or procedural reasons. Another solution would be to cross-check or double-check the activities of authorized persons. This would, however, lead to doubling wage costs and simultaneously creating of investment costs associated with modifying access points (e.g. software application authentication processes or physical access points such as lock systems or card readers).

Another disadvantage of standard measures for monitoring and evaluating the activities of authorized persons is that in many cases they cannot detect the potential identity theft of a person with access rights. According to statistics from 2017 (Gooden, 2017), 85% of intrusions into buildings and sites is facilitated by identity theft.

The deficiencies mentioned above, or limitations of standard protective measures can be minimized by applying **innovative technologies** based on recognizing discrepancies in the real-time behaviour of individuals. This may include, for example, intelligent video analysis by security cameras or analysis of user activity in the information system (e.g. from logs or mouse-movements on the screen). The monitoring system learns the common patterns of behaviour of individual authorized persons and can—in real-time—evaluate each time a person enters the site or information system whether their behaviour differs from their usual patterns. An intelligent system could take advantage of the innovative deep machine learning methods (LeCun et al., 2015), which function similarly to how a child learns. At each additional access, it analyses an individual's movements and learns to assign different details in those movements (locomotion), for example, how they show or swipe their identification card as they pass through a scanned area (such as a turnstile), or mouse movements on a screen. If these details differ significantly, it alerts a relevant authorized person of discrepancies in the usual pattern of behaviour, which may, for example, indicate a possible identity theft (i.e. when an unauthorized person impersonates a person with access rights). Changes in behaviour may also be due to other factors such as medical issues or the ingestion of alcohol or drugs. As well as security, the use of this method has long been applied to disaster and crisis management (Zagorecki et al., 2013).

At present, the most powerful deep learning systems are based on convolutional neural networks (Ciresan et al., 2011) that form a part of the input information process. These neural networks consist of layers of small computing units, so-called neurons, which send the processed information in a hierarchical manner. When convolutional neural networks are trained in the context of a recognition process, they create a representation of information whose complexity grows progressively in the hierarchical process. For example, in VSS/CCTV systems, the first layer determines where light and dark are in the input image. The next determines the edges, other shapes, consequent objects (e.g. humans) or individual types of objects (e.g. man or woman) in an overall assessment of the situation and subsequently to an overall understanding of its meaning (e.g. the position and movements of the person in the scene).

In the case of applying the deep learning method to standard technical measures in a physical or cyber environment, they can be

**Table 6**
Standard technical resources for monitoring and evaluating the activities of authorized persons.

| Physical environment | Cyber environment |
|---|---|
| Video surveillance system (VSS) | Intrusion detection system (IDS). |
| Access control systems (ACS): Logical anti-passback, timed anti-passback, area controlled anti-passback. | Intrusion prevention systems (IPS). |
| Intrusion and hold-up alarm systems (I&HAS). | Intrusion detection and prevention systems (IDPS). |
| GPS tracking and monitoring system. | Information leak detection and prevention (ILDP). |
| Polygraph. | Information leak prevention (ILP). |
| | Content monitoring and filtering (CMF). |
| | Information protection and control (IPC). |
| | Extrusion prevention system (EPS). |
| | Data loss prevention (DLP). |
| | 2FA – Two factor authentication. |

referred to as behavioural biometric systems. In these systems, several measurable quality indicators can be monitored: FAR – False Acceptance Rate, FRR – False Rejection Rate, EER – Equal Error Rate (Lovecek et al., 2015). From the point of view of breaking this measure, the most relevant parameter is FAR, which expresses the likelihood that a biometric security system will incorrectly accept an unauthorized access attempt (Benaliouche and Touahria, 2014). Nowadays, manufacturers of standard technical measures already have this data included in their products.

Deep learning can accurately identify patterns in data and refine them step by step. Once a pattern can be unambiguously assigned to a human identity, it can be considered a behavioural biometric feature. The biometric matching algorithm (which is not necessarily related to deep learning but may be based on a neural or convolutional neural network) for determining a particular pattern of behaviour and identity has a FAR and FRR curve. The risk of accepting an unauthorized person depends on the threshold value set to the level where an identity is already considered the same. This threshold expresses certain FAR and FRR values. The higher the threshold, the lower the risk that an unauthorized person will be granted access. The risk that an authorized person will not be accepted also increases, however.

Indeed, the use of deep learning in security is quite new. Research results in this area have only been available for the past few years. The innovative nature of the issue (i.e. deep learning and the proposed procedures themselves) is demonstrated by the ever-growing number of international scientific publications in the field (Fig. 2).

Obtaining accurate data requires longer-term analysis of statistical data, but in any case, the application of this method has increased significantly, as deep learning is much more accurate and quicker than any other method (Dai and Braytont, 2017; Al-Waisy et al., 2017; Zhu et al., 2017).

The application of new tools such as machine learning or deep learning to existing standard technical resources (Table 6) can provide new options for protective measures. These new measures will then be able to more effectively monitor and evaluate not only the activities but also the behaviour of authorized persons and therefore prevent potential personnel threats.

## 8. Conclusion

Personnel threats, especially intentional threats in the EPCI sector, represent a serious risk to entire critical infrastructure systems. The effect of these threats leads to undesirable events that could result in disruptions or temporary failures in any given element's performance and consequently lead to large electrical power outages. These outages have far-reaching impacts, not only on society itself but also on the dependent critical infrastructure sectors and elements. These sectors are in particular: water supply, health services, information and communication systems, financial market and currency, and public administration.

An important preventive measure leading to the early identification of weak or even critical locations is assessing the resilience of EPCI elements to personnel threats. This assessment is based on the assessment of measurable items in twelve basic areas that determine the basic components of resilience, i.e. robustness, recoverability and adaptability. The result of this evaluation is the classification of measurable items into five categories characterizing the achieved level of resilience (i.e. high, acceptable, low, insufficient and critical level).

From the results of this assessment, adequate security measures for minimizing personnel threats can be adopted by a critical infrastructure owner or operator (i.e. the owner or operator of a given critical Infrastructure element). These measures may be of a procedural, cultural or technical nature. The essence of implementing procedural measures is to define the requirements for individual areas of personnel security, for example, responsibilities, obligations and rights, employee screening, data protection agreements, work performance conditions, employee training, responses to security incidents and failures, disciplinary processes, termination of employment relationships, etc. The essence of implementing cultural measures is to raise employee awareness and interest in security. Technical measures include the use of standard technical resources for monitoring and evaluating the activities of authorized persons (e.g. intruder and hold-up alarm systems or GPS localization systems) and the development of innovative technologies based on, for example, recognizing discrepancies in the behaviour of individuals in real-time through machine learning and deep learning methods.

Identifying weak and critical locations to protect against a personnel threats and the suitable implementation of adequate security measures will lead to a significant reduction in personnel risks and threats and the strengthening of EPCI security. This approach would also significantly contribute to stabilizing the functions of dependent sectors in a critical infrastructure system. In conclusion, although the article is focused on

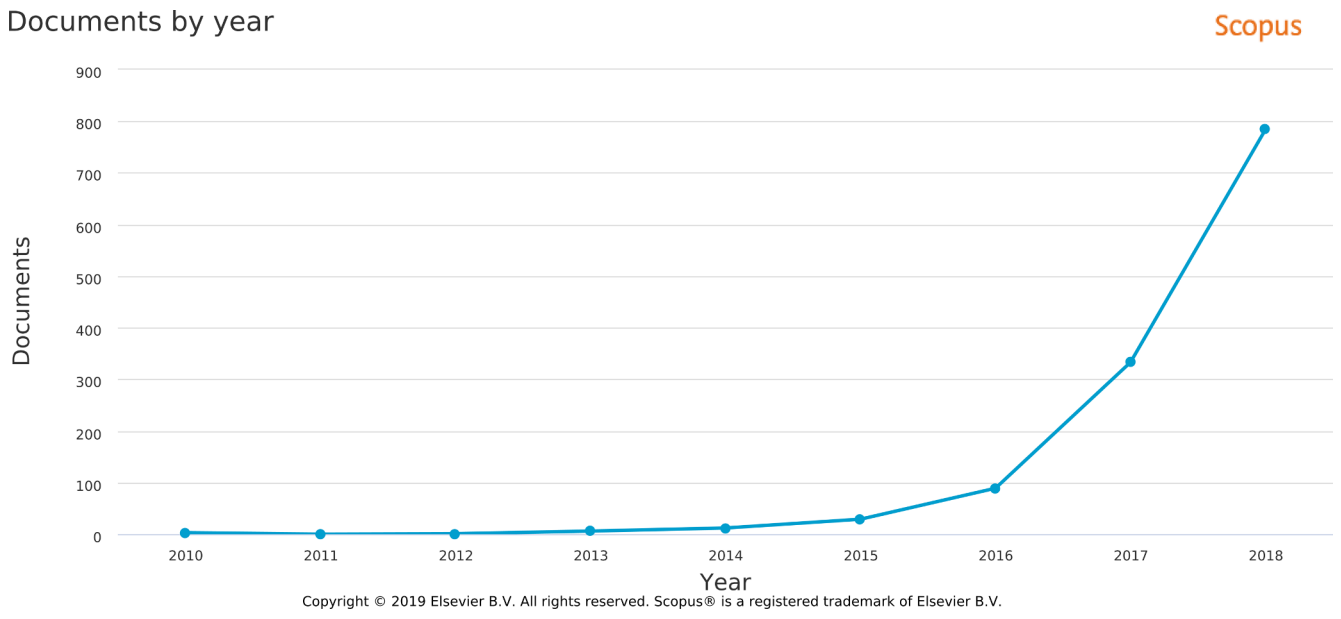


**Fig. 2.** Number of SCOPUS deep learning publications in the context of security.

the context of the Czech Republic, the proposed procedures are fully applicable to any electricity system operator.

## Acknowledgments

This work was supported by the Ministry of the Interior of the Czech Republic, [Grant No. VI20152019049: Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems].

## Declaration of Competing Interest

None.

## References

Act 240 of 28 June 2000 on the crisis management.
Act 458 of 29 December 2000 on business conditions and public administration in the energy sectors and on amendment to other laws (Energy Act).
Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., 2017. A multimodal biometrie system for personal identification based on deep learning approaches. Seventh International Conference on Emerging Security Technologies (EST) 163–168. https://doi.org/10.1109/EST.2017.8090417.
BBC, 2005. Massive power outage in Indonesia. BBC News, British Broadcasting Corporation, London. http://news.bbc.co.uk/2/hi/asia-pacific/4162902.stm (Feb. 27, 2018).
Benaliouche, H., Touahria, M., 2014. Comparative study of multimodal biometric recognition by fusion of iris and fingerprint. Sci. World J., Article ID 829369. doi: 10.1155/2014/829369.
Brown-Cohen, J., 2010. Cascading power failures. In: Laughlin, R.B. (Ed.), Introduction to the Physics of Energy. Standford University, Stanford, CA.
Brvnistan, M., 2016. Security awareness in the context of combating modern security threats. Ninth International Scientific Conference Security Forum 2016, 520–527.
Ciresan, D.C., Meier, U., Masci, J., Gambardella, L.M., Schmidhuber, J., 2011. Flexible, high performance convolutional neural networks for image classification. In: Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence. AAAI Press, Menlo Park, CA, pp. 1237–1242.
Cox, S., Cox, T., 1991. The structure of employee attitudes to safety: a European example. Work Stress 5 (2), 93–106. https://doi.org/10.1080/02678379108257007.
Dai, Y.Y., Braytont, R.K., 2017. Circuit recognition with deep learning. IEEE International Symposium on Hardware Oriented Security and Trust (HOST) 162. https://doi.org/10.1109/HST.2017.7951826.
Deloitte Advisory, 2017. Methodology to ensure of critical infrastructure protection in the area of electricity generation, transmission and distribution. Deloitte Advisory, Prague, Czech Republic (in Czech).
European Council, 2008. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. European Union, Brussels, Belgium.
Garcia, M.L., 2007. The Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann, Oxford, United Kingdom.
Gooden, A., 2017. National Identity Crime Operational Lead UK Policing & Identity Security Adviser to Home Office UK Government Dept. “Quote to BehaVer”. Message to prof. Martin Haran. August 14, 2017.
Halaj, M., Kutaj, M., Boros, M., 2018. The organization's safety culture, its indicators and its measurement capabilities. CBU International Conference on Innovations in Science and Education 595–600. https://doi.org/10.12955/cbup.v6.1219.
Hale, A.R., 2000. Culture's confusions. Saf. Sci. 34, 1–14. https://doi.org/10.1016/S0925-7535(00)00003-5.
Holling, C.S., 1973. Resilience and stability of ecological systems. Ann. Rev. Ecol. Syst. 4, 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245.
IAEA, 1991. Safety Culture: A Report by the International Nuclear Safety Advisory Group. International Atomic Energy Agency, Vienna, Austria.
Jang, S.S., Kwan, S.W., Yoo, H.S., Kim, J.S., Yoon, W.K., 2009. Development of a vulnerability assessment code for a physical protection system: systematic analysis of physical protection (SAPE). Nucl. Eng. Technol. 41 (5), 747–752. https://doi.org/10.5516/NET.2009.41.5.747.
Knake, R.K., 2017. A Cyberattack on the U.S. Power Grid. Council on Foreign Relations, New York, NY. https://www.cfr.org/report/cyberattack-us-power-grid (Jan. 29, 2018).
LeCun, Y., Bengio, Y., Hinton, G., 2015. Deep learning. Nature 521, 436–444. https://doi.org/10.1038/nature14539.
Lovecek, T., Ristvej, J., Simak, L., 2010. Critical infrastructure protection systems effectiveness evaluation. J. Homeland Security Emergency Manage. 7https://doi.org/10.2202/1547-7355.1613. Article 34.
Lovecek, T., Velas, A., Durovec, M., 2015. Security Systems - Alarm Systems. University of Zilina, Zilina, Slovak Republic.
Mikellidou, C.V., Shakou, L.M., Boustras, G., Dimopoulos, Ch., 2018. Energy critical infrastructures at risk from climate change: A state of the art review. Saf. Sci. https://doi.org/10.1016/j.ssci.2017.12.022 (Article in press).
MIT, 2014. Crisis management type plan for the large-scale disruption of electricity supply. Ministry of Industry and Trade, Prague, Czech Republic (in Czech).
Mohamed, S., 2003. Scorecard approach to benchmarking organizational safety culture in construction. J. Construct. Eng. Manage. 129 (1), 80–88. https://doi.org/10.1061/(ASCE)0733-9364(2003)129:1(80).
Morgan, M.G., et al., 2012. In: Terrorism and the electric power delivery system. National Academy of Sciences, Washington, DC. https://doi.org/10.17226/12050.
NIAC (National Infrastructure Advisory Council), 2009. Critical Infrastructure Resilience Final Report and Recommendations. The Department of Homeland Security, Washington, DC.
NEI, 2015. Chernobyl Accident and Its Consequences. Nuclear Energy Institute, Washington, DC. https://www.nei.org/Master-Document-Folder/Backgrounders/Fact-Sheets/Chernobyl-Accident-And-Its-Consequences (Feb. 22, 2018).
Oulehlova, A., 2017. Identification of the electricity blackout impacts on the environmental security. In: Proceedings of the 26th Annual International Conference on European Safety and Reliability (ESREL). CRC Press-Taylor & Francis Group, Boca Raton, FL, pp. 2175–2182.
PPD-21, 2013. Presidential Policy Directive – Critical Infrastructure Security and Resilience. The White House, Washington, DC.
Rehak, D., Markuci, J., Hromada, M., Barcova, K., 2016. Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. Int. J. Crit. Infrastruct. Protect. 14, 3–17. https://doi.org/10.1016/j.ijcip.2016.06.002.
Rehak, D., Senovsky, P., Hromada, M., Pidhaniuk, L., Dvorak, Z., Lovecek, T., Ristvej, J., Leitner, B., Sventekova, E., Maris, L., 2018. Methodology of the Critical Infrastructure Elements Resilience Assessment. VSB – Technical University of Ostrava, Ostrava, Czech Republic (in Czech).
Rehak, D., Senovsky, P., Hromada, M., Lovecek, T., 2019. Complex Approach to assessing resilience of critical infrastructure elements. Int. J. Crit. Infrastruct. Protect. 25, 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003.
Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001. Identifying, understanding and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 21 (6), 11–25. https://doi.org/10.1109/37.969131.
RISKAN, 2015. Risk Support Tool. T-Soft, Prague, Czech Republic. http://www.tsoft.cz/en (Apr. 18, 2018).
Sugden, A.M., 2001. Resistance and resilience. Science 293 (5536), 1731. https://doi.org/10.1126/science.293.5536.1731b.
Ward, D.M., 2013. The effect of weather on grid systems and the reliability of electricity supply. Climatic Change 121 (1), 103–113. https://doi.org/10.1007/s10584-013-0916-z.
Zagorecki, A.T., Johnson, D.E.A., Ristvej, J., 2013. Data mining and machine learning in the context of disaster and crisis management. Int. J. Emergency Manage. 9 (4), 351–365. https://doi.org/10.1504/IJEM.2013.059879.
Zhu, J., Zheng, H., Liao, S., Lei, Z., Cai, C., Zheng, L.X., 2017. Deep hybrid similarity learning for person re-identification. IEEE Trans. Circ. Syst. Video Technol. 3183–3193. https://doi.org/10.1109/TCSVT.2017.2734740.